Application No. 09/685,285

REMARKS

The Applicants and the undersigned thank Examiner Ha for her time and consideration given during the telephone interview of June 7, 2006. The Applicants also appreciate Examiner Ha's careful review of this application. Claims 1-9 and 11-65 have been rejected. Upon entry of this amendment, Claims 1-9 and 11-65 remain pending in this application. Claim 10 has been cancelled without prejudice to or disclaimer of the subject matter contained therein.

The independent claims are Claims 1, 42, 51, and 56. Consideration of the present application is respectfully requested in light of the above amendments to the application and in view of the following remarks.

Summary of Telephonic Interview of June 7, 2006

The Applicants and the undersigned thank the Examiner for her time and consideration given during the telephonic interview of June 7, 2006. During this telephonic interview, proposed amendments to the claims were discussed.

The Applicants' representatives explained that the prior art of record, especially U.S. Patent No. 6,070,190 issued to Reps et al. (hereinafter the "Reps" reference) does not provide any teaching of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat, as recited in amended independent Claims 1, 42, 51, and 56. Furthermore, the Reps reference does not provide any teaching of automatically suggesting a computer security threat procedure or tool based on a classification of the computer security incident information, as recited in amended independent Claims 1, 42, and 56.

The focus of the interview was to make sure that Examiner Ha was comfortable with the new language of the claims and that she understood what inventive features the Applicants are trying to claim. Examiner Ha acknowledged the changes and that she understood the new language. Examiner Ha verified that support for the claim amendments was located in the specification at page 45, lines 3-7.

The Applicants and the undersigned request Examiner Ha to review this interview summary and to approve it by writing "Interview Record OK" along with her initials and the date next to this summary in the margin as discussed in MPEP § 713.04.

-14-

Claim Rejections under 35 U.S.C. §§ 102(e) and 103(a)

The Examiner rejected Claims 1-2 and 4-9, and 11-65 under 35 U.S.C. § 102(e) as being anticipated by the Reps reference. The Examiner rejected Claim 3 under 35 U.S.C. § 103(a) as being obvious in view of the Reps reference in view of a printed publication entitled, "Signed and Delivered: An Introduction to Security and Authentication: Find Out How the JAVA security API can Help You Secure Your Code," authored by Todd Sundsted and published on December 1, 1998 (hereinafter the "Sundsted" reference). The Applicants respectfully offer remarks to traverse these pending rejections.

Independent Claim 1

The rejection of Claim 1 is respectfully traversed. It is respectfully submitted that the Reps and Sundsted references fail to describe, teach, or suggest the combination of (1) recording computer security incident information with at least one of a date and time stamp, the computer security incident information indicating one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat; (2) classifying the computer security incident information; (3) automatically suggesting a computer security threat procedure based on a classification of the computer security incident information; (4) providing data to enable display of the computer security threat procedure comprising one or more steps for one of investigating and responding to the computer security incident information; (5) receiving a selection of one or more steps of the computer security threat procedure; (6) executing the selected one or more steps of the computer security threat procedure; (7) in response to executing the one or more steps of the selected procedure, recording executed computer security threat procedure information and results of the executed one or more steps of the computer security threat procedure with at least one of a date and time stamp; and (8) outputting a record comprising the computer security incident information, executed computer security threat procedure information, results of one or more steps of the executed computer security threat procedure, an identity of a user who selected the computer security threat procedure, and at least one of a corresponding date stamp and time stamp, as recited in amended Claim 1.

The Reps Reference

The Reps reference describes technology that is in the field of network system service, and particularly to an end-user based application availability and response monitoring and alerting system. The technology described by the Reps reference enables the monitoring of availability of response time or other desired performance metrics of an application program from the perspective of an end-user utilizing an application program over a distributed computing network. See the Reps reference, column 1, lines 24-31.

The Reps reference explains that a server computer 202 having an application program 203 provides application services to a client computer system 106 in which the client computer system 106 records information related to the performance of the services of the application program 203 via an application probe software 201 residing on the client computer system 1-6. See Figure 2 reproduced below and in column 5, lines 17-22 of the Reps reference.

FIG.2
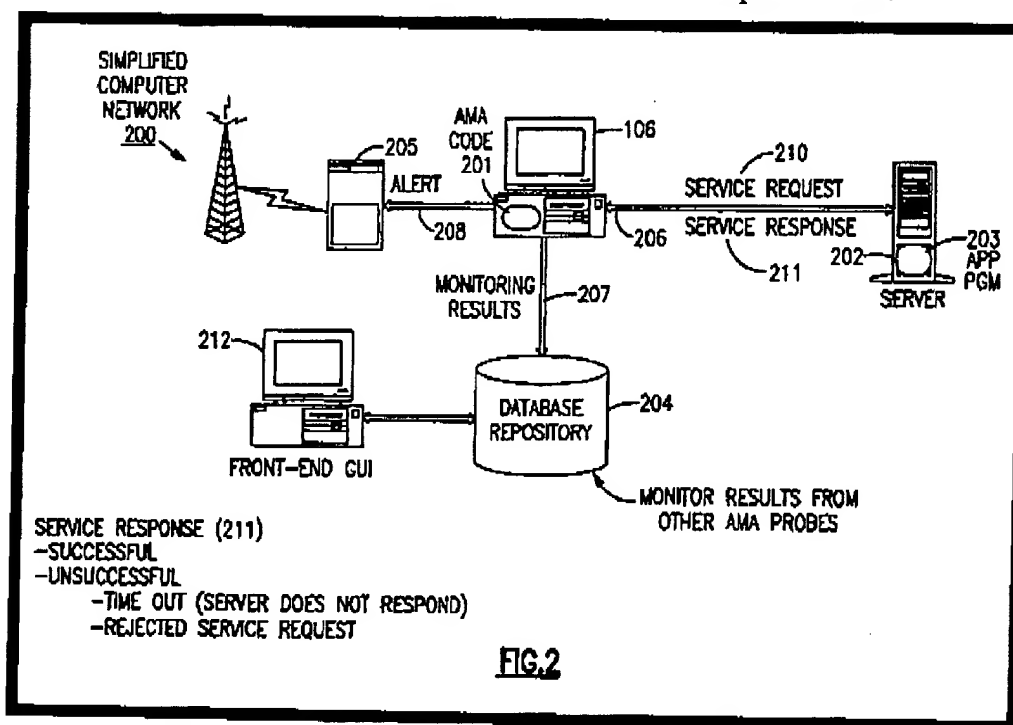
Specifically, as illustrated in Figure 2 above, an application monitoring alerting (AMA) probe 201 can establish a session with a server computer 202 by requesting the services of an application program 203 operating on the server computer 202 through a service request 210. The server computer's application program 203 provides a service response 211 over a network link 206 back to the requesting AMA probe 201. See the Reps reference, column 9, lines 58-68.

-16-

As noted in Figure 2, there are three types of service responses 211 transmitted back to the requesting AMA probe 201 from the server computer 202. First, if the application program 203 on the server computer 202 properly responds to the service request, the AMA probe 201 will receive an indication of a successfully completed request i.e., a successful service response, from the server computer 202. Secondly, if the server computer 202 is unavailable to respond to the service request 210, the request will timeout after a predetermined period and the AMA probe 201 will record that the server computer was not available, and indicate this as an unsuccessful service response. Finally, if the server computer 202 rejects the service request 210, the AMA probe will again record the transaction as an unsuccessful service response 211. See the Reps reference, column 10, lines 29-45.

Whether it is successful or unsuccessful, the service response 211 from the application program 203 on the server computer 202 (including the determination of a no-response time-out) is received at the AMA probe 201, which then records the results of the transaction in a database repository 204. See the Reps reference, column 10, lines 52-57.

The Reps reference does not provide any teaching of recording computer security incident information with at least one of a date and time stamp in which the computer security incident information indicates one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat. Instead of computer security incident information, the Reps reference is primarily concerned with the level of service and performance of an application program 203 residing on a server 202. The Reps reference merely records the response 211 from the application program 203, whether the service request 210 was successful or unsuccessful. The Reps reference is not concerned with why a service request 210 may not have been successful. However, the Examiner believes that the Reps reference teaches some aspects of computer security incident information.

To support the Examiner's finding that the Reps reference teaches some aspects of computer security incident information, the Examiner directs the Applicants' attention to Column 14, lines 55-57 of the Reps reference as set forth on page 3, paragraph 5 of the Final Office Action. However, these passages only discuss performance criteria associated with a level of service:

-17-

"This would be the case, for example, wherein alerting of violation of performance criteria is desired from the probe or wherein only real time transaction information is of interest to the network administrator." Reps reference, column 14, lines 55-57.

Furthermore, the Reps references discloses additional examples of "computer security incidents" including violations of the performance criteria of "threshold information such as maximum response time or minimum application availability" (Col. 24, lines 62-63); a server computer that was recorded as not available (Col. 10, lines 40-41); or an unsuccessful service response (Col. 15, lines 40-41).

One of ordinary skill in the art recognizes that the passages above from the Reps reference do not address computer security incident information indicating one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat. Opposite to monitoring computer security incident information, the Reps reference provides a tool to diagnose and fix programs that are not running properly or in an optimal manner. The Reps reference is not at all concerned with any type of computer security threat or suspicious activity comprising one or more attacks received from a network computer that occur prior to a computer security threat.

The Examiner explains in her Response to Arguments section on page 17, paragraph 1, of the Non-Final Office Action that she is interpreting the term "computer security incident" very broadly. However, the Applicants believe that the Examiner is overlooking how computer security incident information has been further defined within each of the independent claims. For example, in independent Claim 1, the "computer security incident information" indicates one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat. One of ordinary skill in the art recognizes that the Reps reference does not teach this type of computer security incident information as explicitly defined in amended independent Claim 1.

Furthermore, the Reps reference does not provide any teaching of automatically suggesting a computer security threat procedure based on a classification of the computer security incident information, as recited in amended independent Claim 1.

-18-

To support the Examiner's finding that the Reps reference teaches some aspects of suggesting a procedure based on the classification of the computer security incident information, the Examiner directs the Applicants' attention to the following passages of the Reps reference:

> "A determination that one of these pre-defined performance criteria has been violated prompts the AMA probe 201 to generate an alert signal 208 which is sent to an alerting mechanism 205, which in turn is designed to inform an appropriate support entity of the violation such that problem determination and remediation steps may be quickly implemented." Reps reference, column 11, lines 31-34.

> "The alerting mechanism 205 may in turn function by signaling the violation to a support person...." Reps reference, column 24, line 66 to column 25, line 1.

> "These tables 1504 include information related to...who is to be informed of the violation [and] how to inform that person (i.e., e-mail, paging, etc.)...." Reps reference, column 25, lines 33-38.

However, the above passage only teaches the notification of a support person when a violation has occurred. Therefore, in the Reps reference, it is the responsibility of a human being to determine the appropriate problem determination and remediation steps in response to a violation. Accordingly, the Reps reference fails to teach automatically suggesting a computer security threat procedure based on a classification of the computer security incident information, as recited in amended independent Claim 1.

Claim 12, which depends upon independent Claim 1, teaches that some of steps of Claim 1 are performed automatically by a program module. In rejecting Claim 12, the Examiner relied on the following passage from the Reps reference:

> "Next in step 403, the probe configuration information is provided to the executable portion of the AMA probe code which uses the information to initiate a series of service requests 210 in step 404 to a monitored application program 203 on a target server computer system 202." Reps reference, column 15, lines 11-15.

The above passages fails to teach fails to teach automatically suggesting a computer security threat procedure based on a classification of the computer security incident information, as recited in amended independent Claim 1. Instead, and as illustrated above with respect to Figure 2, the passage teaches that after receiving probe configuration , the AMA probe code 201 on the

client computer system 106, initiates a service request 210 to the server computer to establish a session with a server computer 202 by requesting the services of an application program 203 operating on the server computer 202. One of ordinary skill in the art recognizes that service requests are not computer security threat procedures or tools.

The Applicants remind the Examiner that for a rejection based upon 35 U.S.C. § 102, MPEP § 2131 (8th Ed., Rev. 4, October 2005) states:

> "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987).

The Applicants submit that the Examiner has not shown that each and every element contained in amended independent Claim 1 is found in the Reps reference. Because the Reps reference does not teach any aspects of a computer security threat or suspicious activity comprising one or more attacks received from a network computer that occur prior to a computer security threat or automatically suggesting a computer security threat procedure, the Applicants submit that this reference fails to teach numerous elements recited in independent Claim 1 and therefore, the Reps reference fails to anticipate amended independent Claim 1.

The Sundsted Reference

The Examiner admits that the Reps reference fails to provide a teaching of a digital signature in connection with results that are recorded by computer system as recited in dependent Claim 3. To make up for this digital signature deficiency, the Examiner relies upon the Sundsted reference.

The Sundsted reference describes a digital signature that can be generated from a message in connection with sending an e-mail message. The Sundsted reference explains that a good digital signature algorithm guarantees that a digital signature can't be forged assuming the private key is secret, and that the signature is good for only the message from which it is generated. See the Sundsted reference, abstract, third paragraph.

While the Sundsted does provide an isolated teaching on digital signatures as understood by one of ordinary skill in the art, similar to the Reps reference, the Sundsted reference does not provide any computer security context. In other words, like the Reps reference, the Sundsted

-20-

PAGE 24/30 * RCVD AT 6/13/2006 1:01:20 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/22 * DNIS:2738300 * CSID:404 572 5134 * DURATION (mm-ss):09-24

reference is not at all concerned with any type of computer security threat or suspicious activity comprising one or more attacks received from a network computer that occur prior to a computer security threat. The Sundsted reference does not provide any teaching for either investigating or responding to computer security incident information.

In light of the differences between Claim 1 and the Reps and Sundsted references, one of ordinary skill in the art recognizes that these prior art references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 1. Accordingly, reconsideration and withdrawal of the rejection of Claim 1 are respectfully requested.

Independent Claim 42

The rejection of Claim 42 is respectfully traversed. It is respectfully submitted that the Reps and Sundsted references, fail to describe, teach, or suggest the combination of (1) classifying the computer security incident information; (2) automatically suggesting one or more computer security threat investigation procedures based on a classification of the computer security incident information; (3) providing data to enable display of the one or more computer security threat investigation procedures for investigating one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat; (4) providing data to enable display of one or more computer security threat response procedures for responding to one of suspicious computer activity comprising on or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat; (5) in response to a selection of a computer security investigation procedure, providing data to enable display of one or more corresponding investigation steps; (6) in response to a selection of a computer security response procedure, providing data to enable display of one or more corresponding response steps; and (7) generating a permanent record comprising computer security incident information, executed investigation step and result information, executed response step and result information, and corresponding date and time stamps, as recited in amended Claim 42.

As noted above with respect to independent Claim 1, neither the Reps reference nor the Sundsted reference relate in any way to suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat or an

-21-

actual computer security threat; as recited in amended Claim 42. Furthermore, neither the Reps reference nor the Sundsted reference relate in any way to automatically suggesting one or more computer security threat investigation procedures based on a classification of the computer security incident information; as recited in amended Claim 42. The Reps reference is merely concerned with logging performance of a computer and ways to diagnose or improve performance. The Sundsted reference provides only a general teaching of digital signatures using private and public keys.

Furthermore, and similar to Claim 1, the Reps reference does not provide any teaching of automatically suggesting one or more computer security threat investigation procedures based on a classification of the computer security incident information, as recited in amended independent Claim 42. As noted with respect to Claim 1, the Reps reference only teaches the notification of a support person when a violation has occurred. Therefore, in the Reps reference, it is the responsibility of a human being to determine the appropriate problem determination and remediation steps in response to a violation.

In light of the differences between Claim 42 and the references mentioned above, one of ordinary skill in the art recognizes that the prior art references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 42. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 51

The rejection of Claim 51 is respectfully traversed. It is respectfully submitted that the Reps and Sundsted references, fail to describe, teach, or suggest the combination of (1) accessing a table comprising computer locations, Internet address ranges associated with the computer locations, and computer security step information associated with the computer locations, (2) the computer security step information for one of investigating and responding to one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat, (3) the computer locations identifying devices that are able to perform computer security steps associated with the computer security step information; (4) comparing a computer security step to be executed and a target Internet address with computer locations and Internet address ranges listed in the table; (5) determining if a match exists between an Internet address of a computer security incident and the

-22-

Internet address ranges listed in the table; and (6) automatically selecting a computer to execute the computer security step based upon the matching step, wherein the computer has a location and is capable of interacting with the Internet address of the computer security incident, as recited in amended Claim 51.

Neither the Reps reference nor the Sundsted reference relate in any way to suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat; as recited in amended Claim 51. The Reps reference is merely concerned with logging performance of a computer and ways to diagnose or improve performance. The Sundsted reference provides only a general teaching of digital signatures using private and public keys. Neither reference provides steps for investigating or responding to suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat or an actual computer security threat.

Furthermore, neither the Reps reference nor the Sundsted reference relate in any way to automatically selecting a computer to execute a computer security step based upon the matching step, wherein the computer has a location and is capable of interacting with the Internet address of the computer security incident; as recited in amended Claim 51. Support for this claim amendment is located in the specification at page 41, line 23 to page 42, line 3.

To support the Examiner's finding that the Reps reference teaches some aspects of selecting a computer to execute a computer security step based upon the matching step, the Examiner directs the Applicants' attention to Column 11, lines 23-65 and Column 25, lines 39-43 of the Reps reference. However, these passages merely teach the notification of a support person with an alert signal when a violation has occurred. Therefore, in the Reps reference, it is the responsibility of a human being to subsequently determine the appropriate problem determination and remediation steps in response to a violation. Accordingly, the Reps reference fails to teach automatically selecting a computer to execute a computer security step based upon the matching step, wherein the computer has a location and is capable of interacting with the Internet address of the computer security incident, as recited in amended independent Claim 51.

The Reps and Sundsted references also do not access a table comprising computer locations, Internet address ranges associated with the computer locations, and computer security step information associated with the computer locations, the computer security step information

-23-

for one of investigating and responding to one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat, and the computer locations identifying devices that are able to perform computer security steps associated with the computer security step information, as recited in independent Claim 51.

To support the Examiner's finding that the Reps reference teaches some aspects of accessing a table comprising computer locations for one of investigating and responding to one of suspicious computer activity, the Examiner directs the Applicants' attention to Column 5, lines 46-48 and Column 11, lines 51-52 of the Reps reference.

> "In an embodiment of the invention these parameters may include such information as the name of the application program, the address of the server system..." Reps reference, column 5, lines 46-48.

> "[T]he probe configuration information 302 will include...the network address of the target server and the type of application on the target server to be monitored...." Reps reference, column 11, lines 48-53.

However, these passages only discuss storing location information to access the application server of the Reps reference. The application server of the Reps reference is not a computer location that is able to perform computer security steps associated with the computer security step information for one of investigating and responding to one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat, as recited in amended independent Claim 51.

In light of the differences between Claim 51 and the references mentioned above, one of ordinary skill in the art recognizes that the prior art references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 51. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

Independent Claim 56

The rejection of Claim 56 is respectfully traversed. It is respectfully submitted that the Reps and Sundsted references, fail to describe, teach, or suggest the combination of (1) receiving

-24-

computer security incident information indicating one of suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat and an actual computer security threat; (2) classifying the computer security incident information; (3) displaying one or more tools for one of investigating and responding to computer security incident information; (4) automatically suggesting a tool based on a classification of the computer security incident information; (5) receiving a selection of a tool; (6) in response to a selection of a tool, forwarding data for execution of the tool; and (7) forwarding data for generating a permanent record comprising computer security incident information, executed tool information, and corresponding date and time stamps, as recited in amended Claim 56.

Neither the Reps reference nor the Sundsted reference relate in any way to suspicious computer activity comprising one or more attacks received from a network computer that occur prior to a computer security threat or an actual computer security threat; as recited in amended Claim 56.

Furthermore, neither the Reps reference nor the Sundsted reference relate in any way to automatically suggesting a tool based on a classification of the computer security incident information, wherein the tools are for one of investigating and responding to computer security incident information. The Reps reference is merely concerned with performance of a computer and ways to diagnose or improve performance. The Sundsted reference provides only a general teaching of digital signatures using private and public keys. Neither reference displays one or more tools for one of investigating and responding to computer security incident information.

To support the Examiner's finding that the Reps reference teaches some aspects of automatically suggesting a tool based on a classification of the computer security incident information, the Examiner directs the Applicants' attention to Column 11, lines 31-34 and Column 25, lines 1-2 and 35-38 of the Reps reference. However, these passages only teach the notification of a support person when a violation has occurred. Therefore, in the Reps reference, it is the responsibility of a human being to subsequently determine the appropriate problem determination and remediation steps in response to a violation. Accordingly, the Reps reference fails to teach automatically suggesting a tool based on a classification of the computer security incident information, as recited in amended independent Claim 56.

-25-

In light of the differences between Claim 56 and the references mentioned above, one of ordinary skill in the art recognizes that the prior art references, alone or in combination, cannot anticipate or render obvious the recitations as set forth in amended independent Claim 56. Accordingly, reconsideration and withdrawal of this rejection are respectfully requested.

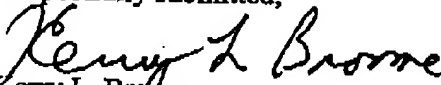### Dependent Claims 2-9, 11-41, 43-50, 52-55, and 57-65

The Applicants respectfully submit that the above-identified dependent claims are allowable because the independent claims from which they depend are patentable over the cited references. The Applicants also respectfully submit that the recitations of dependent Claims 2-9, 11-41, 43-50, 52-55, and 57-65 are of patentable significance. Accordingly, reconsideration and withdrawal of the rejections of the remaining dependent claims are respectfully requested.

CONCLUSION

The foregoing is submitted as a full and complete response to the Office Action mailed on March 13, 2006. The Applicants and the undersigned thank Examiner Ha for the consideration of these remarks. The Applicants have submitted remarks to traverse the rejections of Claims 1-9 and 11-65. The Applicants respectfully submit that the present application is in condition for allowance. Such Action is hereby courteously solicited.

If any issues remain that may be resolved by telephone, the Examiner is requested to call the undersigned at 404.572.4647.

Respectfully submitted,

Kerry L. Broome
Reg. No. 54,004

King & Spalding LLP
34th Floor
1180 Peachtree Street, N.E.
Atlanta, Georgia 30309
404.572.4600
K&S Docket: 05456.105008

-26-